

JAN 08 2007

67,108-043
Wong 1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Wong, Marcus
Serial No.: 09/827,226
Filed: April 5, 2001
Group Art Unit: 2136
Examiner: Shiferaw, Eleni, A.
Title: SYSTEM AND METHOD FOR PROVIDING SECURE
COMMUNICATIONS BETWEEN WIRELESS UNITS USING
A COMMON KEY

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Appellant now submits its brief in this appeal. The Commissioner is authorized to charge Deposit Account No. 50-1482 in the name of Carlson, Gaskey & Olds in the amount of \$500.00. The Commissioner is authorized to charge Deposit Account No. 50-1482 in the name of Carlson, Gaskey & Olds for any additional fees or credit the account for any overpayment.

Real Party in Interest

Lucent Technologies, Inc. is the Assignee of record of this application.

Related Appeals and Interferences

There are no related appeals or interferences.

01/10/2007 EFLORES 00000034 501482 09827226

01 FC:1402 500.00 DA

BEST AVAILABLE COPY

RECEIVED
CENTRAL FAX CENTER

JAN 08 2007

67,108-043
Wong 1**Status of the Claims**

Claims 21-40 are rejected under 35 USC 102 and are on appeal. Claims 1-20 have been cancelled.

Status of Amendments

There are no unentered amendments.

Summary of Claimed Subject Matter

The claims on appeal are directed to methods of providing secure communications between wireless units that use session keys and a common key value to provide secure communications between the wireless units.

Independent claim 21 recites:

21. A method of providing secure communications between a first wireless unit that uses a first session key and a second wireless unit that uses a second session key, the method comprising:

generating a common key value as a function of at least a portion of at least one of the first session key or the second session key; and

providing the common key value to the first wireless unit for use in secure communications between the first wireless unit and the second wireless unit having the common key value.

Figure 3 schematically shows one example method of providing secure communications between a first wireless unit 80 that uses a first session key CK1 and a second wireless unit 82 that uses a second session key CK2 (page 11, lines 7-8 and 27-28; page 12, lines 2-3).

A common key value CKC is generated as a function of at least a portion of at least one of the first session key CK1 or the second session key CK2. Depending on the embodiment, the common key value CKC can be generated in different ways. Some key generation techniques use the session keys CK1 and CK2 or portions thereof as inputs. (Page 12, lines 7-9)

The common key value is provided to the first wireless unit 80 for use in secure communications between the first wireless unit 80 and the second wireless unit 82 having the

67,108-043
Wong 1

common key value CKC. Once the common key value CKC is generated and is ready to be distributed to the first and second wireless units 80 and 82 in the illustrated example, the first wireless communications system 84 sends the common key value CKC encrypted using the session key CK1 to the first wireless unit 80. (Page 14, lines 4-7)

Independent claim 33 recites:

33. A method of communication using a first wireless unit for communicating with a second wireless unit;

receiving at the first wireless unit, a common key value that is a function of at least a portion of at least one of a first session key associated with the first wireless unit or a second session key associated with a second wireless unit; and

using the common key value for secure communications between the first wireless unit and the second wireless unit.

Figure 3B is useful for understanding an embodiment upon which claim 33 reads. A first wireless unit 80 is used for communicating with a second wireless unit 82. The first wireless unit 80 receives a common key value CKC that is a function of at least a portion of at least one of a first session key CK1 associated with the first wireless unit 80 or a second session key CK2 associated with a second wireless unit 82. In the example of Figure 3B, the first wireless communication system 84 sends the common key value CKC encrypted using the session key CK1 to the first wireless unit 80. The first and second wireless units 80 and 82 now can communicate securely using the common key value CKC as the common encryption/decryption key (page 14, lines 8-9).

Grounds of Rejection to be Reviewed on Appeal

Claims 21-40 were rejected under 35 U.S.C. §102(b) as being anticipated by "Dynamic Participation in a Secure Conference Scheme for Mobile Communications, Min-Shiang Hwang, IEEE Transactions on Vehicular Technology, Vol. 48, No. 5, September 1999. For discussion purposes, this document will be referred to as "the Hwang '99 reference."

67,108-043
Wong 1

Claims 21 and 33 were rejected under 35 U.S.C. §102(b) as being anticipated by "Scheme For Secure Digital Mobile Communications Based on Symmetric Key Cryptography," Tzonelih Hwang, IEEE, Region 10 Conference, Tencon 92, 1992. For discussion purposes, this document will be referred to as "the Hwang '92 reference."

ARGUMENT

There is no *prima facie* case of anticipation. Neither of the references relied upon by the Examiner includes a method that involves generating a common key value as a function of at least a portion of a session key associated with a wireless unit. Instead, as explained below, both references relied upon by the Examiner use a random number as a common key. A random number, by definition, is random and is not a function of a session key. Therefore, there is no anticipation.

The Hwang '99 reference does not anticipate any of Claims 21-40.

The Hwang '99 reference does not disclose a common key value that is a function of at least a portion of a session key associated with a wireless unit. Beginning on page 1470, the Hwang '99 reference teaches a key distribution protocol. The text uses NC to indicate a network center, T_i to indicate a personal terminal used by a user U_i , r_i to indicate a session key-decryption key used by each terminal T_i and CK to indicate a common secret session key of a secure teleconference that is chosen randomly by the NC. (see, e.g., Hwang '99, p. 1470, col. 1, lines 18-19) As indicated on page 1471, col. 1, lines 8-9, the network center NC "chooses nonzero random numbers CK and r_0 , CK being a common secret session key of the secure conference."

The Examiner improperly interprets the common key CK of the Hwang '99 reference as if it were generated as a function of the session keys r_i used by each termination T_i . Step 7 of the

67,108-043
Wong 1

Hwang reference on page 1471 clearly indicates that the network center NC chooses *nonzero random* numbers CK. Those random numbers are not a function of any portion of the session keys r_i used in the Hwang '99 reference. Therefore, the Examiner's interpretation of the Hwang '99 reference is not reasonable. It is not a reasonable interpretation to consider a random number to be a function of another number when the random number is simply selected as a random number. If it were a function of the other numbers, it would cease to be random. Moreover, there is nothing in the Hwang '99 reference that indicates that the common key CK is generated by the NC as a function of any other number, let alone the session keys r_i selected by the terminals T_i .

There is no anticipation and the rejection under 35 U.S.C. §102(b) based upon the Hwang '99 reference must be reversed.

The Hwang '92 reference does not anticipate either of Claims 21 or 33.

The relevant portion of the Hwang '92 reference begins on page 423. The most relevant portion is on page 424, which describes the scheme used in the Hwang '92 reference. The following is a quotation:

When user i at a terminal desires to have a secure communication with a second user j at a second terminal, user i generates a nonce, n_1 , and sends n_1 to user j.

Upon receiving the message, user j generates a nonce, n_2 , and sends both n_1 as well as n_2 to the network center. Knowing that both user i and j want to have a secure communication, the center generates a random number, SK, which serves as the session key.

While the Hwang '92 reference discloses sending more information than the random number SK to the user i, that additional information does not somehow transform the random number SK into a function of a session key or nonce in this case. The random number SK is just that – a random number. There is nothing else in the Hwang '92 reference that would be considered similar to a common key value as recited in Applicant's

RECEIVED
CENTRAL FAX CENTER

JAN 08 2007

67,108-043
Wong 1

claims. Assuming that the Examiner interprets the nonces as the "session keys" and the random number SK as the "common key value", the random number SK is not a function of the nonce n_1 or the nonce n_2 . Therefore, it is an unreasonable interpretation of the reference to construe the nonces to be the same as the session keys associated with wireless units and the session key SK to be the same as the common key value of Applicant's claims. Therefore, there is no anticipation.

CONCLUSION


Neither of the references relied upon by the Examiner disclose generating a common key value as a function of at least a portion of at least one session key associated with a wireless unit. Instead, both references disclose using a random number (i.e., a random number common key CK or a random number session key SK). There is nothing more in either reference other than a straightforward statement that the random numbers are generated as random numbers. There is no reasonable interpretation of either reference that can establish a *prima facie* case of anticipation against any of Applicant's claims. The rejections must be reversed.

Respectfully submitted,

CARLSON, GASKEY & OLDS, P.C.

January 8, 2007

Date



David J. Gaskey
Registration No. 37,139
400 W. Maple, Suite 350
Birmingham, MI 48009
(248) 988-8360

RECEIVED
CENTRAL FAX CENTER

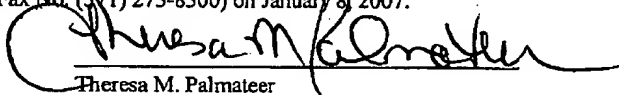
007/014

JAN 08 2007

67,108-043
Wong 1

CERTIFICATE OF FACSIMILE

I hereby certify that this Appeal Brief, relative to Application Serial No. 09/827,226 is being facsimile transmitted to the Patent and Trademark Office (Fax No. (571) 273-8300) on January 8, 2007.



Theresa M. Palmateer

N:\Clients\LUCENT TECHNOLOGIES\IP00043\PATENT\Appeal Brief 1-8-07.doc

67,108-043
Wong 1**APPENDIX OF CLAIMS**

1-20. (Cancelled)

21. A method of providing secure communications between a first wireless unit that uses a first session key and a second wireless unit that uses a second session key, the method comprising:

generating a common key value as a function of at least a portion of at least one of the first session key or the second session key; and

providing the common key value to the first wireless unit for use in secure communications between the first wireless unit and the second wireless unit having the common key value.

22. The method of claim 21, comprising

sending the common key value to the first wireless unit using the first session key.

23. The method of claim 22, comprising

sending the common key value to the second wireless unit using the second session key.

67,108-043
Wong 1

24. The method of claim 23, comprising
encrypting the common key value with the second session key; and
transmitting the encrypted common key value to the second wireless unit.
25. The method of claim 22, comprising
encrypting the common key value using the first session key; and
transmitting the encrypted common key value to the first wireless unit.
26. The method of claim 21, comprising
generating the first session key as a function of a first root key known only at the first
wireless unit and a wireless communication system accessed by at least the first wireless unit.
27. The method of claim 21, comprising
generating the second session key as a function of a second root key known only at said
second wireless unit and at a home wireless communication system accessed by at least said
second wireless unit.
28. The method of claim 21, comprising
generating the common key value as a function of the first session key and the second
session key.

67,108-043
Wong 1

29. The method of claim 21, comprising
generating the common key value as an encryption key.
30. The method of claim 21, comprising
generating the common key value as a session key.
31. The method of claim 21, comprising
mutually generating the common key value by a first wireless communication system
accessed by the first wireless unit and a second wireless communication system accessed by the
second wireless unit.
32. The method of claim 21, comprising
using the common key value for a first communication session between the first and
second wireless units; and
using the same common key value for a second, different communication session between
the first and second wireless units.

67,108-043
Wong 1

33. A method of communication using a first wireless unit for communicating with a second wireless unit;

receiving at the first wireless unit, a common key value that is a function of at least a portion of at least one of a first session key associated with the first wireless unit or a second session key associated with a second wireless unit; and

using the common key value for secure communications between the first wireless unit and the second wireless unit.

34. The method of claim 33, comprising

generating the first session key corresponding to the first wireless unit; and

obtaining the common key value by said first wireless unit using said first session key.

35. The method of claim 34, comprising

decrypting the common key value using the first session key.

36. The method of claim 34, wherein

the first session key is generated as a function of a first root key known only at the first wireless unit and a wireless communication system accessed by at least the first wireless unit.

67,108-043
Wong 1

37. The method of claim 33, comprising
using the common key as an encryption key.
38. The method of claim 33, comprising
using the common key as a session key.
39. The method of claim 33, wherein the common key value is a function of the first session
key and the second session key.
40. The method of claim 33, comprising
using the common key value for a first communication session between the first wireless
unit and the second wireless unit; and
using the same common key value for a second, different communication session between
the first wireless unit and the second wireless unit.

67,108-043
Wong 1

EVIDENCE APPENDIX

None.

67,108-043
Wong 1

RELATED PROCEEDINGS APPENDIX

None.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.